UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,852	09/12/2003	Mandayam Thondanur Raghunath	YOR920030222US1	8538

24299 7590 07/24/2007

GEORGE SAI-HALASZ
303 TABER AVENUE
PROVIDENCE, RI 02906

EXAMINER	
TRAN, ELLEN C	
ART UNIT	**PAPER NUMBER**
2134	
MAIL DATE	**DELIVERY MODE**
07/24/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

70

Office Action Summary	**Application No.** 10/661,852	**Applicant(s)** RAGHUNATH ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4-14,16 and 18-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1, 2, 4-14, 16, and 18-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to communication filed on: 2 May 2007 with acknowledgement of an original application filed on 12 September 2003.

2. Claims 1, 2, 4-14, 16, and 18-20 are pending; claims 1, 4, 10, and 20 are independent claims. Claims 1, 2, 10, and 16, have been amended; claims 3, 15, and 17 have been canceled. Amendments to the claims are accepted.

Response to Arguments

3. Applicant's arguments filed 2 May 2007 have been fully considered however they are moot due to new grounds of rejection.

In addition Examiner notes the Applicant failed to address the 35 U.S.C. 101 rejection in the first Office Action and repeated below directed to claim 20. Appropriate correction is required, such as canceling claim 20.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claim 20 is rejected under 35 U S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 20 is directed to carrier wave signal, which is not patentable subject matter.

6. To expedite a complete examination of the instant application the claims rejected under 35 U.S.C. 101 (nonstatutory) are further rejected as set forth below in anticipation of applicant amending these claims to place them within the four statutory categories of invention.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. **Claims 1, 4-8, 10-14, and 18-20,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Oskari U.S. Patent Publication No. 2006/0072755 (hereinafter '755) in view of Kung U.S. Patent 5,442,342 (hereinafter '342).

As to independent claim 1, "A portable computing device for opening a door, comprising: a memory, wherein a content of the memory comprises: a first copy of a shared secret key; a first standard certificate, wherein the first standard certificate is being used in responding to a challenge of the door" is taught in '755 page 3, paragraphs 0052-0053;

"and means for communicating with the door, wherein the door possesses a second copy of the shared secret key, and wherein the door adapted to validate identicalness of the first and the second copies of the shared secret key" is shown in '755 page 3, paragraphs 0058-0061;

the following is not explicitly taught in '755:

"and wherein the door further adapted to issue the challenge on randomly selected occasions to the computing device" however '342 teaches that the third aspect of the invention of protecting a distributed computer system is to generate the challenges to the system at random times in col. 2, lines 39-41.

It would have been obvious to one of ordinary skill in the art at the time of a wireless lock and key system using an encryption key pair taught in '755 to include a means to generate challenges at random times. One of ordinary skill in the art would have been motivated to perform such a modification to improve security see '342 (col. 2, lines 1 et seq.) "Accordingly, there is a need for a foolproof means of recognizing and authenticating an authorized user in a computer system".

As to independent claim 4, "A method for secure unlocking of a door based on a shared secret key, comprising the steps of: providing a portable computing device, wherein the computing device is equipped with a memory, and the memory holds a first copy of the shared secret key and a first standard certificate, wherein the computing device is adapted for performing operations with shared secret keys and standard certificates," is taught in '755 page 3, paragraphs 0052-0053;

"and wherein the computing device is also having means for communicating with the door communicating by the computing device to the door a device identifier; issuing a challenge by the door to the computing device" is shown in '755 page 3, paragraphs 0058-0061;

"responding to the challenge by the computing device by demonstrating possession of a private key part of the first standard certificate" is disclosed in '755 page 3, paragraphs 0052-0053;

"responding by the door with a door identifier and with a message, wherein the message is encrypted with a second copy of the shared secret key, and wherein using the second copy of the shared secret key for encrypting the message resulted from recognizing

the device identifier communicated by the computing device" is shown in '755 page 5, paragraphs 0119-0122;

"responding by the computing device with a signal attesting decryption of the message, wherein the message has been decrypted in the computing device by the first copy of the shared secret key, and wherein using the first copy of the shared secret key for decrypting the message resulted from recognizing the door identifier transmitted by the door; and unlocking the door upon recognizing validity of the signal attesting decryption of the message" is shown in '755 page 5, paragraphs 0119-0122;

the following is not explicitly taught in '755: **"wherein the challenge is issued only on randomly selected occasions"** however '342 teaches that the third aspect of the invention of protecting a distributed computer system is to generate the challenges to the system at random times in col. 2, lines 39-41.

It would have been obvious to one of ordinary skill in the art at the time of a wireless lock and key system using an encryption key pair taught in '755 to include a means to generate challenges at random times. One of ordinary skill in the art would have been motivated to perform such a modification to improve security see '342 (col. 2, lines 1 et seq.) "Accordingly, there is a need for a foolproof means of recognizing and authenticating an authorized user in a computer system".

As to dependent claim 5, "wherein the device identifier is a hash code of the first standard certificate" is taught in '355 page 7, paragraphs 0134-0135.

As to dependent claim 6, "wherein the door identifier is a simple identifier and it is sent without encryption" is shown in '355 page paragraph 3, paragraphs 0052 and 0070 note the lock device identifier having a human readable name is interpreted to be without encryption, this identifier is obviously sent when the unencrypted random number is signaled with the challenge in paragraph 0052.

As to dependent claim 7, "wherein the door has a second standard certificate, and the door identifier is a hash code of the second standard certificate" is disclosed in '755 page 7, paragraph 0139.

As to dependent claim 8, "wherein the shared secret key is generated by the door and communicated with the computing device in private using a public key part of the first standard certificate" is taught in '755 page 3, paragraphs 0052-0053.

As to independent claim 10, "A security system for controlling access, comprising a first plurality of doors and a second plurality of portable computing devices for opening doors each computing device equipped with a memory, wherein any one of the computing devices holds in its memory a unique first standard certificate and wherein the any one computing device further holds in its memory door identifiers for all those doors out of the first plurality of doors that the any one computing device is permitted to open" is disclosed in '755 page 3, paragraphs 0062-0071;

"and wherein each of the door identifier is uniquely linked to a first copy of a shared secret key, wherein any one of the doors possesses a matching information for each one of those computing devices out of the second plurality of computing devices that are permitted to open the any one door, wherein the matching information comprises a device identifier, wherein the device identifier is linked to a public key part of the unique first

standard certificate and to a second copy of the shared secret key" is taught in '755 page paragraphs 0052-0053;

"and wherein the first plurality of doors and the second plurality of computing devices have means for communicating between any device and any door, and wherein the any one door is adapted to recognize the device identifier, and further adapted to use the matching information to validate identicalness of the first and the second copies of the shared secret key" is shown in '755 page 3, paragraphs 0058-0061;

the following is not explicitly taught in '658: **"and to issue a challenge on randomly selected occasions to the unique first standard certificate using the public key part of the unique first standard certificate"** however '342 teaches that the third aspect of the invention of protecting a distributed computer system is to generate the challenges to the system at random times in col. 2, lines 39-41.

It would have been obvious to one of ordinary skill in the art at the time of a wireless lock and key system using an encryption key pair taught in '755 to include a means to generate challenges at random times. One of ordinary skill in the art would have been motivated to perform such a modification to improve security see '342 (col. 2, lines 1 et seq.) "Accordingly, there is a need for a foolproof means of recognizing and authenticating an authorized user in a computer system".

As to dependent claims 11-13, these claims contain substantially similar subject matter as claims 5-7; therefore they are rejected along similar rationale.

As to dependent claim 14, "wherein the door identifier is a hash code of the unique second standard certificate" is taught in '355 page 7, paragraphs 0134-0135.

As to dependent claim 15, "wherein the challenge is issued on randomly selected occasions" however '342 teaches that the third aspect of the invention of protecting a distributed computer system is to generate the challenges to the system at random times in col. 2, lines 39-41.

As to dependent claim 18, "wherein the challenge by the any one door is successfully responded by demonstrating possession of a private key part of the unique first standard certificate" is shown in '755 page 3, paragraph 0052-0053.

As to dependent claim 19, "wherein the any one door is further adapted to generate a shared secret key and communicate the shared key in private by using the public key part of the unique first standard certificate" is disclosed in '755 page 3, paragraphs 0052-0053.

As to independent claim 20, this claim is directed to a computer data signal that incorporates the limitation of the method of claim 4; therefore it is rejected along similar rationale.

9. **Claims 2, 9, and 16,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Oskari U.S. Patent Publication No. 2006/0072755 (hereinafter '755) in view of Kung U.S. Patent 5,442,342 (hereinafter '342) in further view of Zuili U.S. Patent No. 7,083,090 (hereinafter '090).

As to dependent claim 2, "wherein the first standard certificate is having a private key part and the private key part is being encrypted with a first biometric key, wherein the first biometric key belongs to a rightful owner of the computing device" is taught in '755 page 3, paragraph 0073;

the following is not explicitly taught in the combination of '755 and '342: **"wherein the computing device further comprising a biometric device, wherein the biometric device is capable of generating a second biometric key"** however '090 teaches the portable smartcards may be provided with a plug-in type biometric device in col. 3, lines 3-9;

"wherein the second biometric key belongs to a user of the computing device, and wherein the second biometric key is used to decrypt the private key part of the first standard certificate" however '090 teaches that the use of the smartcard can be prevented if the fingerprint does not correspond to the authorized user, obviously if the user is authorized the sensed fingerprint would be used to decrypt the private key part of the first certificate in col. 3, lines 26-30.

It would have been obvious to one of ordinary skill in the art at the time of a wireless lock and key system that uses challenges generated at random times taught in '755 and '342 to include a means to utilize biometrics. One of ordinary skill in the art would have been motivated to perform such a modification to improve security while being scalable to existing infrastructures see '090 (col. 1, lines 43 et seq.) "Accordingly, the need remains for a system which allows the use of these alternative devices, including portable devices, while, at the same time, provides a level of security, scalability and transparency in conjunction with existing infrastructures which is at least as good, and preferably much higher, than systems currently in use".

As to dependent claim 9. "wherein the private key part of the first standard certificate is encrypted with a first biometric key, wherein the first biometric key belongs to a rightful owner of the computing device" is taught in '755 page 3, paragraph 0073;

"and wherein the computing device is provided with a biometric device, and wherein the step of responding to the challenge further comprise the steps of: taking a biometric reading of a user of the computing device" however '090 teaches the portable smartcards may be provided with a plug-in type biometric device in col. 3, lines 3-9;

"generating a second biometric key using the biometric reading; and decrypting the encrypted private key part of the first standard certificate using the second biometric key, whereby if the first and second biometric keys are identical the decrypting using the second biometric key is successful, and the challenge can be successfully responded" however '090 teaches that the use of the smartcard can be prevented if the fingerprint does not correspond to the authorized user, obviously if the user is authorized the sensed fingerprint would be used to decrypt the private key part of the first certificate in col. 3, lines 26-30.

As to dependent claim 16, "wherein the unique first standard certificate is having a private key part and the private key part is being encrypted with a first biometric key, wherein the first biometric key belongs to a rightful owner of the computing device" is taught in '755 page 3, paragraph 0073;

"wherein the any one computing device is further comprising a biometric device, wherein the biometric device is capable of generating a second biometric key" however '090 teaches the portable smartcards may be provided with a plug-in type biometric device in col. 3, lines 3-9;

"wherein the second biometric key belongs to a user of the any one computing device, and wherein the second biometric key is used to decrypt the private key part of the first standard certificate" however '090 teaches that the use of the smartcard can be prevented if the fingerprint does not correspond to the authorized user, obviously if the user is authorized the sensed fingerprint would be used to decrypt the private key part of the first certificate in col. 3, lines 26-30.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran

Ellen Tran
Patent Examiner
Technology Center 2134
18 July 2007